UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In re SONY BMG CD TECHNOLOGIES LITIGATION	:	Civil Action No. 1:05-cv-09575-NRB
	:	CLASS ACTION
This Document Relates To:	:	DECLARATION OF STEVEN M. BELLOVIN IN SUPPORT OF THE RICCIUTI CLASS REPRESENTATIVES' MOTION FOR AN AWARD OF ATTORNEYS' FEES AND REIMBURSEMENT OF EXPENSES
ALL ACTIONS.	:	

I, STEVEN M. BELLOVIN, declare as follows:

1. I am an expert in the area of computer security, retained by the plaintiffs' attorney in the above-captioned litigation. I am a professor of computer science. Attached hereto as Exhibit A is a true and correct copy of my résumé. I have knowledge of the matters stated herein and, if called upon, I could and would competently testify thereto.

2. I have reviewed the Settlement Agreement entered into between the plaintiffs and defendant dated December 28, 2005. I have estimated the impact as follows:

3. An attacker who wishes to take over a computer system faces three problems: initial penetration, concealment of the attack, and (under some circumstances) gaining sufficient privileges on that computer to carry out further attacks or tasks. The XCP software aids in the second of these problems; the MediaMax software aids in the third and in some cases the second. In addition, at least one version of an uninstaller for the XCP software was a significant aid in the first of the attacker's problems.

4. The XCP software installs a so-called rootkit. The purpose of a rootkit is to conceal other software running on a computer. Rootkits are often used by malware to hide from the system administrator and probably from anti-virus software. In this case, Sony employed the rootkit to hide its own DRM software, presumably to prevent its removal by the system owner administrator. However, there was no mechanism to prevent it from concealing other, more malicious software; according to published reports (*see* http://news.zdnet.co.uk/internet/security/0,39020375,39236720,00.htm and http://www.vnunet.com/vnunet/news/2145874/virus-writers-exploit-sony-drm), at least two pieces of malicious software were modified to do exactly that.

5. The MediaMax software creates a file that is executed any time a protected CD is played. In and of itself, this is not a problem; however, the file is created in such a fashion that any user of the computer, even one without "privileges", can overwrite this file and hence replace it with a modified version. Consider, for example, a home computer where a parent or older child, running on a privileged account, regularly plays protected CDs. A younger child, running on an unprivileged account – one that does not have privileges to modify, say, a protective Internet filter – could use this security hole to gain privileges. This would allow that child to remove filtering software, examine confidential documents such as tax returns, etc.

6. In addition, if there were some system penetration by a mechanism that did not grant full privileges – consider this child inadvertently downloading a worm or visiting a Web site that exploited a browser flaw – the attacker could use this same whole to gain full privileges on the system.

7. Under certain circumstances, the MediaMax software could be abused to help with the initial penetration of the computer. If a consumer were to share a computer's drive over a home network, other computers on that network – perhaps having been penetrated by some other mechanism – could exploit this vulnerability to overwrite that file. The next time the owner played a protected CD, the malicious version of the file will be executed.

8. Some components of the Sony-installed software "phone home," apparently whenever the album is played. Although the apparent purpose is to check for updates to the art work or lyrics (http://www.sysinternals.com/blog/2005/11/more-on-sony-dangerous-decloaking.html), it is also an invasion of privacy. To start, it tells Sony each time the album is played. Beyond that, they learn the IP address of the customer. IP addresses tend to disclose the location of the sender (http://www.zabasearch.com/frames/zaba_location.map.php). Beyond that, IP addresses are

effectively static for many broadband Internet users. Sony can thus build a profile of albums played by customers. They can also correlate this IP address with logs from their other web sites, all without the permission of the customer.

9. It is harder to assess the actual, as opposed to potential, impact. It is, however, well-known that the computer underground values compromised machines for their profit-making potential; *see,* for example, http://news.zdnet.com/2100-1009_22-5772238.html?tag=nl. Machines that are "disinfected" are of no use; accordingly, any mechanism that keeps the "bot" intact, such as a rootkit, is quite valuable.

10. Compromised machines that are turned into bots are used to send spam and to launch denial of service attacks as a form of extortion. If an ISP detects such behavior, its general response is to disable the affected account. The consumer is thus denied all Internet access for some time.

11. It is notoriously difficult to thoroughly disinfect compromised machines. The difficulty is, of course, exacerbated if a rootkit conceals the offending files. The most common advice is to reinstall the operating system; if not done extremely carefully, this can result in a loss of all data and personal files on the machine. A typical reinstallation, including downloading and installing all Microsoft patches and reinstalling all application programs, can take the better part of a day, even if there are no problems. Resolving problems often requires calls to Help Desks and/or costly professional assistance. Microsoft itself has noted the need for reinstallation, especially if the malware is taking advantage of rootkits to conceal its presence (http://www.eweek.com/article2/0,1895,1945808,00.asp).

12. The XCP rootkit is particularly difficult to uninstall. As noted in http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html, errors in uninstalling it can render a system unbootable, disable the CD drive, and more. The author notes

"most users that stumble across the cloaked files with a RKR scan will cripple their computer if they attempt the obvious step of deleting the cloaked files." Indeed, Sony's original uninstaller itself posed very serious security risks (http://www.freedom-to-tinker.com/?p=926). The flaws in it were detected by outsiders, not by Sony itself; for this reason, the provision in the settlement for outside, official review is quite crucial.

13. The total number of infected computers around the world is not known; however, it is very large. A recent Dutch arrest involved a botnet of at least 1.5 million computers (http://news.com.com/Bot+herders+may+have+controlled+1.5+million+PCs/2100-7350_3-5906896.html). As noted above, one of the challenges facing someone who wants to operate a large botnet is concealing the infestation. A rootkit makes this task much easier.

I declare under penalty of perjury that the foregoing is true and correct. Executed this 6th day of April, 2006, at Westfield, New Jersey.

STEVEN M. BELLOVIN

T:\CasesSF\Sony NY\DEC00029673.doc